السنة: الخامسة المجلد: 05 العدد: 01 ص ص: 789 - 816
EISSN 2676-1645 ISSN 2543-375X

السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية: الصين نموذجا
National Cyber Sovereignty under Cyberspace and Digital Transformation: china's model

فاطمة بيرم [1] جامعة قسنطينة 3
fatima.birem@univ-constantine3.dz

تاريخ الإرسال: 2019/09/16 تاريخ القبول: 2019/11/24

ملخص:

يناقش المقال طبيعة العلاقة بين الفضاء السيبراني وسيادة الدولة، حيث لطالما ارتبط المفهوم التقليدي للسيادة الوطنية لقرون مضت بعوامل تقليدية لها صلة وثيقة بالجغرافيا. لكن مع تطور الاتصالات، حدثت تغيرات هائلة في مفهوم السيادة وبات من الصعب القطع بفكرة السيطرة المطلقة على المعلومات في ظل الارتباط والاندماج بالشبكة الدولية للمعلومات التي أضحت أحد أبرز عوامل القوة السياسية من جهة، وعناصر ضعف الدول من جهة أخرى.

بناءا على ذلك برز مفهوم "السيادة السيبرانية" التي تؤطر معايير السيادة في عصر المعلومات، فلم يعد الأمر مقتصرا على المحيط الجغرافي أو المائي أو حتى الجوي للدول، بل عملت وسائل الاتصال الحديثة على خلق فضاء جديد يختلج كميات كبيرة من المعلومات التي تخص الأمن القومي لدول العالم، وفي ظل هذا التحول الرقمي المتسارع أصبح مفهوم السيادة السيبرانية أمرا غاية في الأهمية لأي دولة في العالم.

لذلك تسعى الصين إلى اعتماد وتوسيع نطاق سيادتها السيبرانية وتخصص لها موارد هائلة خاصة الصناعات الالكترونية، وذلك لإنشاء فضاء تتحكم فيه وطنيا الأمر الذي يخرجها شيئا فشيئا من دائرة الهيمنة والاحتكار الذي تمارسه الشركات الأمريكية في هذا المجال، غير أنه لا يمكن إرجاع دوافع

[1]- المؤلف المراسل

تبني الصين لسيادتها في الفضاء السيبراني إلى بعد واحد فقط، بل هي أبعاد: سياسية، اقتصادية، أمنية، ثقافية، وأخرى مرتبطة بالتطلعات العالمية الصينية.

الكلمات المفتاحية:

الفضاء السيبراني- السيادة السيبرانية- الدولة- الأمن القومي- الصين.

Abstract :

The article discusses the nature of the relationship between cyberspace and state sovereignty, where this concept has long been associated with traditional factors closely related to geography. But with the development of communications, there have been many changes in the concept of sovereignty and it is difficult to control absolutly information because of the connectivity of the international information network, which has become one of the most important factors of political power, and also the elements of state weakness.

Consequently, the concept of “cyber sovereignty” is no longer confined to the geographical, water, or even airspace of states. With this accelerated digital transformation, the concept of national cyber sovereignty has become critical to any country in the world.

Therefore, China seeks to adopt its cyber sovereignty and expand its scope by allocating huge resources, especially in the domain of electronic industries, to create a national-controlled space, which is slowly getting out of the circle of hegemony and monopoly exercised by American companies in this field, However, the motives for China's adoption of its sovereignty in cyberspace can not be resumed just in one dimension, but are political, economic, security, cultural, and other related to China's global aspirations.

keywords: Cyberspace - Cyber sovereignty - State - National Security - China.

مقدمة:

يشهد المجتمع البشري تطورا مطردا في مجال التكنولوجيا الرقمية وتطبيقاتها، لتغدو معه حياة الإنسان أكثر ارتباطا بالأجهزة الالكترونية والعوالم الافتراضية، كما جاءت التكنولوجيا الرقمية لتلقي بجل تأثيرها على

تطور الأنظمة السياسية، وتشكيل العلاقات الدولية، فعلى الرغم من الايجابيات التي حملتها، إلا أنها حملت معها العديد من التهديدات والمخاطر على كافة المستويات سواء أفراد، مؤسسات أو دول.

وقد طغى هذا المشهد على السيادة القومية للدول، حيث أوجدت التطورات التكنولوجية الهائلة ساحات سيادية جديدة دفعت دول العالم لفرض رقابتها الأمنية عليها، لذلك أصبح الأمن السيبراني أحد أهم أركان منظومة الأمن القومي لمعظم دول العالم.

فمفهوم سيادة الدول لم يعد كما استقر عليه قبل المستحدثات التكنولوجية الجديدة التي لا تعترف بحدود دولية، فباتت الدول تخشى منها على سيادتها وبالتالي أمنها القومي الذي بات قابل للاختراق في ظل التهديدات الجديدة ذات الطبيعة السيبرانية.

لذلك يدعو المشهد الالكتروني العالمي في عصر الثورة التقنية والمعلوماتية إلى الوقوف على حدود التفاعل الرقمي القائم بين الفضاء السيبراني والسيادة والأمن القومي لدول العالم، في ظل انصهار الحدود الجغرافية للدول، نتيجة التطورات التكنولوجية التي أتاحت للدول إمكانية الولوج في فضاء إلكتروني يحوي العديد من عناصرها ومعلوماتها القومية والأمنية والاقتصادية والسياسية...الخ.

وتعتبر الصين الدولة الأبرز في هذا المجال، حيث تسعى جاهدة للاعتراف بسيادتها في هذا الفضاء، ويُعد هذا المفهوم جزءا أساسيا لفهم الإستراتيجية الصينية الجديدة. فعبر القوانين المحلية والابتكارات التقنية والسياسة الخارجية، تهدف الصين لبناء نظام دفاع سيبراني "عصيّ على الاختراق"، وبالتالي إعادة صياغة الفضاء السيبراني وفقًا لما تتخيله، وهو ما يتعارض مباشرة مع الدعم الأمريكي لمبدأ الفضاء السيبراني العالمي المفتوح.

وعليه نطرح إشكالية الدراسة كالتالي:

ما هي دوافع الاهتمام الصيني بالسيادة الوطنية في الفضاء السيبراني؟

وللإلمام والخوض في الإجابة على هذا التساؤل المحوري وجب علينا صياغة التساؤلات الفرعية التالية:

ما هو مفهوم الفضاء السيبراني؟

ما هو مفهوم السيادة السيبرانية؟

ما هي طبيعة العلاقة بين الفضاء السيبراني وسيادة الدول؟ وهل يمكن سحب مفهوم السيادة ليشمل هذا الفضاء؟

كيف وظفت الصين سيادتها السيبرانية لخدمة مصالحها المختلفة؟

ولسهولة تفكيك الإشكالية المطروحة، نبني الفرضية التالية:

تسعى الصين إلى اعتماد سيادتها السيبرانية، وذلك لتوظيف قدراتها في الفضاء السيبراني، لمجابهة الهيمنة الالكترونية الغربية -الأمريكية-، بما يضمن أقل التكاليف المادية والبشرية ويُحقق أهدافها الإستراتيجية المختلفة.

أولا: الفضاء السيبراني: المفهوم والدلالات

1- مفهوم الفضاء السيبراني:

جاء الفضاء السيبراني ليدخل كمجال خامس جديد في العلاقات الدولية العابرة للحدود والقادرة على امتلاك منصات القوة الشاملة، سواء من قبل الفاعلين من الدول أو من غير الدول، وهو يمثل امتدادا لنشاط الإنسان ذي الطابع المدني أو العسكري، ويوازي ما يقوم به الإنسان في المجالات والفضاءات الدولية الأخرى، كالمجال البري والبحري والجوي والفضاء الخارجي.

انبثقت عبارة "cyber" من أعمال "نوربرت واينر norbert weiner" الذي قدم تعريفا لعبارة "cybernetics" في منتصف القرن العشرين، مفادها أن التفاعل بين الإنسان والآلة يؤدي إلى خلق بيئة بديلة للاتصال، تشكل البنى الأساسية لمفهوم الفضاء السيبراني (عبد الصادق، 2016، ص07).

وفي أوائل الثمانينات صاغ الكاتب وليام غيبسون "william Gibson" عبارة cyber space في رواياته عن المستقبل حيث وصف الفضاء السيبراني بأنه "هلوسة رضائية، يمارسها يوميا بلايين المستخدمين في كل الأوطان...فهو تعقيد فاق التصور" (عراجي، 2016، ص08). وبالتالي فالفضاء السيبراني عنده ليس فضاء بيانات ساكنة لكن قنواته الاتصالية تصل العالم الحقيقي وتتيح لمستخدمي هذا الفضاء سبل التفاعل مع ذلك العالم. رغم أن العبارة

وضعت في سياق الخيال العلمي، إلا أنها أصبحت تستخدم بشكل واسع بين الأكاديميين والمتخصصين في هذا المجال، خاصة مع ظهور وانتشار الانترنت وتعميم استخدام الرقمنة.

وفي أوائل تسعينيات القرن الماضي وضع "جان بيري بارلو John Perry Barlow" العبارة كمفهوم معاصر في سياق وصفه للعلاقة بين الكمبيوترات، وشبكات الاتصال السلكية واللاسلكية، وقد وصف الفضاء السيبراني بأنه وطن بلا حدود، متحديا بذلك فكرة الدولة القومية، مميزا بذلك بين عالم افتراضي وعالم واقعي(عراجي، ص 08). فالفضاء السيبراني مجال افتراضي من صنع الإنسان يعتمد على نظم الكمبيوتر وشبكات الانترنت وكم هائل من البيانات والمعلومات والأجهزة.

كما عرفته الوكالة الفرنسية لأمن أنظمة الإعلام المكلفة بالدفاع السيبراني الفرنسي بأنه: "فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية."(Kempf, 2015, p09)

أما القاموس العسكري لوزارة الدفاع الأمريكية فقد عرَّف الفضاء السيبراني بأنه: "حقل عالمي في بيئة المعلومات المؤلفة من شبكة مترابطة من البيانات والبنى التحتية لتكنولوجيا المعلومات، تضم: شبكة الانترنت، شبكات الاتصال، الحواسيب، أنظمة المعالجة والتحكم."

كل هذه التعاريف السابقة ركزت على الجانب التقني وأهملت العامل البشري الذي يعد جزءا أساسيا في فهم الفضاء السيبراني. وقد جاء تعريف "الاتحاد الدولي للاتصالات" أشمل باعتباره الفضاء السيبراني: "المجال المادي وغير المادي الذي يتكون وينتج عن عناصر عدة هي: أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل والتحكم، ومستخدمو كل هذه العناصر". (https://bit.ly/2JBgWe8)

وبالتالي يعد الفضاء السيبراني عبارة عن فيض رقمي من المعلومات لا يعتمد كليا على البيئة المحوسبة التي توفرها شبكات المعلومات، بل تتعامل أيضا بكثافة مع مفرداته مثل سرعة تناقل البيانات وصلاحية الدخول إلى الشبكة،

بالإضافة إلى المعالجات التي تتناول البيانات المتدفقة ضمن البيئة السيبرانية. (عبد الصادق، ص11)

ويتكون الفضاء السيبراني من المكون الأول المادي الذي يتمثل في الأسلاك والمحولات والبنية التحتية المعلوماتية: كالكابلات "Hard Ware"، والمكون الثاني يتمثل في المحتوى المعنوي والذي يعكس شكل المعلومات في الفضاء السيبراني "Soft Ware"، أما المكون الثالث فيتمثل في عملية التوصيل بين المعلومات والبشر وحركة التفاعل مابين البرمجيات والمعدات، وارتباط ذلك بتصورات وقيم وسلوك المستخدمين من البشر(عبد الصادق، ص12).

وقد أصبح الفضاء السيبراني أحد العناصر الأساسية التي تؤثر في النظام الدولي، بما يتيحه من أدوات تكنولوجية مهمة لعمليات الحشد والتعبئة في العالم، فضلا عن التأثير في القيم السياسية، فسهولة الاستخدام ورخص التكلفة زاد من قدرته على التأثير في مختلف مجالات الحياة، سواء السياسية، الاقتصادية، العسكرية، الاجتماعية...الخ، وبات جليا أن من يمتلك آليات توظيف البيئة السيبرانية يصبح أكثر قدرة على تحقيق أهدافه والتأثير في سلوك الفاعلين المستخدمين لهذه البيئة.

فإلى وقت قريب كان الفضاء السيبراني يعتبر من مسائل "السياسات الدنيا"، وهي عبارة تستخدم للدلالة على الشؤون الاجتماعية والاقتصادية، التي لا تؤثر بشكل جذري في استقرار الدولة، أما اليوم فإنه أصبح من مسائل "السياسات العليا"، فممارسات كقطع الانترنت في فترات عدم الاستقرار لدولة ما، أو تسريب وثائق حكومية سرية، أو هجوم سيبراني، كلها أمثلة تدل على أنه لا يمكن تجاهل وجود وقدرات الفضاء السيبراني (عراجي ص14).

وبالتالي نظرا لاختلافات استخدامات الفضاء السيبراني المدنية والعسكرية، الأمر الذي استوجب ضرورة التحول من الفوضى إلى التنظيم لعمليات الاستخدام المتعددة له، وهو ما يتطلب البحث عن مسارات متكاملة تحقق هذا الهدف، والتي منها ما يتعلق بالأبعاد التقنية والسياسية والاقتصادية والقانونية وغيرها، للعمل على تنظيم الاستخدام السلمي للفضاء السيبراني وتحقيق التوازن بين الاستخدامات والواجبات. ويأتي هذا بعد أن شهد العالم

تطورا في المخاطر الأمنية مع تطور مراحل النضج التكنولوجي، وأصبحت قضية أمن الفضاء السيبراني تلقى اهتماما متصاعدا على أجندة الأمن الدولي، وذلك في ظل انتشار مصطلحات مثل، الدفاع السيبراني، الهجوم السيبراني، الجريمة السيبرانية، الإرهاب السيبراني...الخ

2- الفضاء السيبراني وحماية الأمن القومي: الأمن السيبراني كرافد جديد

يقصد بالأمن السيبراني مجموع الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به، وسوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظم المعلومات، وتأمين حماية وسرية البيانات الشخصية ولحماية المواطنين. (https://bit.ly/2LWHhFb)

أما الاتحاد الدولي للاتصالات فيعرف الأمن السيبراني: بأنه مجموع الأدوات والسياسات، وضوابط الأمن والمبادئ التوجيهية، ونهج إدارة المخاطر والإجراءات والتدريب، وأفضل الممارسات وآليات الضمان والتكنولوجيات، التي يمكن استخدامها في حماية البيئة السيبرانية وأصول المؤسسات والمستعملين، وتشمل أصول المؤسسات والمستعملين أجهزة الحوسبة الموصولة بالشبكة، والموظفين، والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات، ومجموع المعلومات المنقولة و/أو المحفوظة في البيئة السيبرانية. (https://bit.ly/2JZHEfN)

وبالتالي فإن الأمن السيبراني ينطوي على حماية شبكات الكمبيوتر والمعلومات التي تحتويها من الاختراق ومن الضرر الخبيث أو التعطيل، وذلك بجعل المعتدين يحجمون عن خططهم، أو منعهم من تحقيقها، وإلى ضمان حد مقبول من الأخطار، وذلك عبر وضع خطة تتلاءم والمحيط التقني، البشري، التنظيمي والقانوني. (https://bit.ly/2JBgWe8)

فالعالم إذن يواجه في العصر التكنولوجي المتطور عددا من التهديدات الأمنية التي تتسم بتغيرها وتطورها المستمر واتساع نطاق تأثيرها وأوسعها انتشارا وهي التهديدات السيبرانية.

فالبيئة التكنولوجية التي أتاحت للدول إمكانية الولوج في فضاء الكتروني ضعيف الأمن وفائقا السرعة، خاصة مع التسارع في تبني الحكومة الالكترونية، واتساع نطاق وعدد مستخدمي الانترنت في العالم، حيث أصبحت قواعد البيانات القومية في حالة انكشاف، مما أدى إلى التأثير في سيادة الدولة والتشكيك في قدرتها على الحفاظ على أمنها القومي(خليفة، 2017، ص 54)،

مما خلق حالة من الخوف وهاجس من الطرف الآخر، خاصة مع التفاوت المعلوماتي والتكنولوجي بين دول العالم. (https://bit.ly/32AYzOe)

وقد بدأ التركيز على الفضاء السيبراني كتهديد أمني جديد بفعل أحداث دولية أهمها أحداث 11 سبتمبر 2001، وذلك مع استخدام تنظيم القاعدة له كساحة قتال ضد الولايات المتحدة، وفي عام 2007 برز بوضوح دور الفضاء السيبراني كمجال جديد في العمليات العدائية في الصراع بين استونيا وروسيا، وفي 2008 في الحرب بين روسيا وجورجيا، وجاء الهجوم السيبراني بفيروس "ستاكنست" على برنامج إيران النووي عام 2010 ليمثل نقلة مهمة بالتطور في مجال الأسلحة الالكترونية.(عبد الصادق، ص11).

هذا إضافة إلى الدور الكبير الذي لعبته شبكات التواصل الاجتماعي في حالة الثورات العربية في بداية 2011، حيث مثلت نقطة هامة في زيادة الاهتمام الدولي بأمن الفضاء السيبراني، وبرزت محاولات للسيطرة عليه بعد تصاعد الاحتجاجات حتى في الدول الأكثر ديمقراطية كبريطانيا والولايات المتحدة.

وبالتالي فقد فرض الفضاء السيبراني إعادة التفكير في مفهوم الأمن القومي، فكلمة أمن أصبحت إذا تشير إلى طيف واسع من المجالات ضمن وخارج حقل تقنية المعلومات. (عبد الصادق، ص12-13).

حيث أصبح لكل بعد محتوى ومجالا أمنيا قوميا لأي دولة في العالم، وجها معلوماتيا ورقميا ينبغي الحفاظ عليه، أهمها ما يأتي:

الأمن القومي العسكري: يعد المحتوى المعلوماتي الرقمي العسكري من أخطر الأبعاد تأثيرا على الأمن القومي، نظرا لحساسية ما يحتويه من معلومات الكترونية عن الجوانب العسكرية والتسلحية للدول، لذلك فإن غالبية

الابتكارات العسكرية والتسلحية تعمل في وقتنا الحاضر من خلال ربطها بوسائل الاتصال الحديثة وشبكات الانترنت، وقواعد البيانات وأنظمة المعلومات العسكرية والحربية، والتي تمكن مستخدميها من التحكم بها عن بعد(محمد الطيب وخنيش، 2018، ص30). وتتعدد الأمثلة الموضحة لذلك من خلال بعض الهجمات والاختراقات أهمها اختراق أنظمة المنشات النووية الإيرانية وتعطيلها عن العمل سنة 2010، وذلك من خلال فيروسين اعتبرا الأقوى والأكثر حيلة وقدرة على الاختراق هما flame وstuxnet، فقد حول الأول الأجهزة الإيرانية إلى آلات تصوير وتسجيل وأوقف العمل في مرفأ "خرج" النفطي، ما أدى إلى فصله عن الشبكة الالكترونية، بينما أوقف الثاني عمل مئات من أجهزة الطرد المركزي في معامل تخصيب اليورانيوم، وتوجهت أصابع الاتهام مباشرة إلى إسرائيل والولايات المتحدة اللتين لم تنفيا التهمة .(https://bit.ly/2XQ5NPq)

الأمن القومي السياسي: يتلخص بالبيانات الرقمية، التي تخص الدولة وأجهزتها السيادية، والمتعلقة بالأحزاب أو البرلمان، أو الحكومة...الخ، وهي معلومات حساسة قد تؤدي إلى مشاكل في حال العبث بها، (محمد الطيب وخنيش، ص30) هدفها زعزعة ثقة الشعب بمؤسسات الدولة، وبالتالي تحويلهم إلى أرضية مواجهة بديلة عن المواجهة المباشرة بين الدول، وهو ما برز بظهور فكرة "إسقاط النظام من الداخل" بدلا من استخدام القوة العسكرية الخارجية (عبد الصادق، ص11).

الأمن القومي الاقتصادي: وهو أكثر القطاعات القومية عرضة للهجمات الالكترونية، حيث باتت المعرفة محرك الإنتاج والنمو الاقتصادي والنهوض بالاقتصاد الوطني، وهو ما دفع الدول لأن تزيد من استثمارها في المعرفة، وأصبحت عصرنة الاقتصاد مرتبطة بالتحكم في الاقتصاد الرقمي، من طرف الفاعلين الاقتصاديين والاجتماعيين، مما زاد من أهمية ضرورة توفير الأمن السيبراني لضمان حماية هذه المعلومات (بارة، 2017، ص 430).

الأمن القومي الاجتماعي الثقافي: أصبح التدفق الحر للمعلومات سلاحا قويا في يد الفواعل المختلفة يمكن من خلاله التأثير في الدول سواء متقدمة أو

نامية، لكن الأثر الأكبر يقع على عاتق الدول النامية، خاصة مع امتلاك القوى الكبرى لوسائل تحقيق ذلك، لأن تدفق المعلومات يجري باتجاه واحد من الغرب إلى الشرق، وذلك لاختراق هذه المجتمعات وزرع القيم والأفكار الثقافية للقوى المسيطرة، والتأسيس لهوية ثقافية للمجتمعات المخترقة بعد إسقاط عناصر الممانعة والمقاومة لديها (جبر، 2015، ص 140).

كل هذه الأمور جعلت السيادة الوطنية على المحك، حيث خلقت ساحات سيادية عديدة للدول، تزاوجت مع التوجهات الاقتصادية والسياسية في العالم، في ظل عالم رقمي تسوده لغة الخطر التكنولوجي والحرب الالكترونية.

ثانيا: الفضاء السيبراني وإعادة تعريف مفهوم السيادة الوطنية

1- مفهوم السيادة السيبرانية

يعود مفهوم السيادة إلى معاهدة وستفاليا عام 1648 التي أرست قاعدة أن يكون للدولة سيادة على أراضيها وشؤونها دون تدخل الدول الأخرى في شؤونها الداخلية، وتعد السيادة من المقومات الأساسية التي بني عليها صرح القانون الدولي المعاصر، ويعد مفهومها من المفاهيم الهامة التي اهتم بها فقهاء القانون وباحثي السياسة على قدم المساواة(أبو هيف، 1995، ص35).

لطالما كانت السيادة ولا تزال محل إشكال وجدل كبير بين المفكرين، وقد طرأ على مفهومها تحولات جمة من مطلق إلى نسبي وذلك ربطا بالتطورات المتلاحقة وما أفرزته من معطيات جديدة.

إن تطور الفضاء السيبراني والتكنولوجيا أحدث تغير كبير في العالم، مما أدى إلى المطالبة بإعادة النظر وتقييم لمبادئ القانون الدولي التقليدي أهمها السيادة.

بناءا على ذلك برز مفهوم "السيادة السيبرانية" التي تؤطر معايير السيادة في عصر المعلومات، حيث وجدت ساحات سيادية جديدة دفعت دول العالم لفرض رقابتها الأمنية عليها، فلم يعد الأمر مقتصرا على المحيط الجغرافي أو المائي أو حتى الجوي للدول، بل عملت وسائل الاتصال على خلق فضاء جديد يختلج كميات كبيرة من المعلومات التي تخص الأمن القومي لدول العالم، وفي ظل

هذا التحول الرقمي المتسارع أصبح مفهوم السيادة الوطنية السيبرانية أمرا غاية في الأهمية لأي دولة في العالم (محمد الطيب وخنيش، ص27).

السيادة السيبرانية هي مفهوم حديث متميز مشتق عن مصطلح الأمن السيبراني الأكثر شيوعا والذي يتعلق بحماية البنية التحتية والعمليات المتصلة بالانترنت، كما سبق وبينا، من ناحية أخرى تهتم السيادة السيبرانية بالمعلومات والمحتوى الذي توفره الانترنت، فهي مفهوم غامض يعرف جدل كبير بين الأكاديميين وحتى السياسيين، فبشكل عام يستخدم غالبا للتعبير عن قوة الدولة واستقلالها في الفضاء السيبراني، وذلك لوصف أشكال مختلفة من الاستقلالية والتحكم والسيطرة على البنى التحتية الرقمية، والتقنيات والمحتويات الرقمية والاتصالات، وكافة الأشياء التي يمكن أن ترتبط بالفضاء السيبراني والتعامل معه (https://bit.ly/2Gj7avd).

ويعد مفهوم "السيادة السيبرانية" جديدا نسبياً، ويمكن تلخيصه ببساطة كدفاع بلد لاستعادة السيطرة على بياناته وبيانات مواطنيه. وفي الجانب العسكري، يشمل ذلك قدرة دولة على تطوير قدرات الأمن السيبراني الهجومية والدفاعية، دون الاعتماد على التكنولوجيا أجنبية الصنع. وفي شقه الاقتصادي، يشمل القضايا التي تمتد من فرض الضرائب على التكنولوجيا الكبيرة إلى إنشاء شركات ناشئة محلية.(https://bit.ly/2SklUyR)

وبالتالي فإن السيادة السيبرانية تعني خضوع الفضاء السيبراني لمصالح وقيم الدولة، أي قدرة الدول على التحكم في مجالها السيبراني بما يضمن أنه يتبع نفس القواعد والمعايير والاعتبارات من بقية المجتمع. فهي عبارة تستخدم في مجال حوكمة الانترنت لوصف رغبة الحكومات في ممارسة السيطرة على الانترنت داخل الحدود الوطنية التابعة لهذه الحكومات، أي أنها تطبيق لحقوق والتزامات سيادة الدول على الفضاء السيبراني.(https://bit.ly/2YcDEkQ)

ومع ذلك فإن طبيعة الفضاء السيبراني – حدوده المخترقة- خلقت تحدي لسيادة الدولة وتثير تساؤلات حول ما إذا كان يمكن تطبيق مبادئ القانون الدولي هذه على الفضاء السيبراني.

إن السيادة الإقليمية أصبحت مفتوحة ومستباحة بفعل التقدم التكنولوجي وأصبح الأقوى تكنولوجيا يتمتع بقدرة فائقة على اكتشاف ما يجري عند الآخرين ومعرفة أدق أسرارهم من دون استئذانهم والأمثلة عديدة على ذلك: كعمليات التصنت، والتجسس، ...الخ، مما أخضع مفهوم السيادة التقليدي للمراجعة وإعادة التعريف من المفهوم المطلق إلى المفهوم المحدود أو النسبي، أي تراجع مبدأ السيادة الوطنية للدول، وقد كان مرد ذلك إلى عدة أمور:

- بروز نوعية من المشكلات الدولية التي تستلزم تكاثف الجهود الدولية في سبيل التوصل إلى حلول ناجعة وفعالة مثل: القرصنة الالكترونية، الحرب الالكترونية...الخ

- الاتجاه المتنامي نحو احترام حقوق الإنسان وحرياته الأساسية، ونحو كفالة الضمانات الدولية التي تمكن احترام هذه الحقوق وتكفل عدم انتهاكها من جانب الحكومات الوطنية. (البزاز، 2002، ص16-17)

- ساهم التطور الهائل في وسائل وتكنولوجيات الاتصال في اختراق سيادة الدول، فلم يعد باستطاعة أية دولة أن تحتكر الإعلام والحفاظ على مقومات هويتها، وذلك بسبب الكم الهائل من الأخبار والمعلومات والأفكار والصور المتدفقة دون شروط أو قيود من خارج حدودها (أبو جودة، 2008، ص108).

- لم يعد في مقدور أية دولة، الاعتماد على الذات فقط والاكتفاء بما تنتج من منتجات المعلوماتية، هذا الوضع حتم على الدولة الاستعانة بغيرها من شركات تكنولوجيا المعلومات، فتقدم صناعة البرامج المعلوماتية فرض على الدولة توسيع دائرة اتصالاتها الخارجية والدخول في أنماط جديدة من الشراكة مع القطاع الخاص، فالتطور العلمي في مجال صناعة برامج الكمبيوتر أفضى بفعل التعقيدات التي أفرزها تراجع دور الدولة التقليدي في المجال العسكري وتصاعد دور شركات الصناعات الحربية.(عراجي، ص85-86)

- وجدت الدولة نفسها أمام صعوبات في فرض قيود على دخول البضائع إليها، حيث أصبح بإمكان الشركات التكنولوجية الكبرى استخدام إعلانات تجارية للمنتجات، دون أن يتم دفع أي رسوم للدولة وهو ما يؤثر على

السوق المحلية، ويعزز احتكارها للخدمات والتكنولوجيا بما يؤثر على الاقتصاد الوطني.

- أحدث الفضاء السيبراني تغييرات في مجال وظائف الدولة، وبخاصة فيما يتعلق بوظيفة الدفاع الخارجية، والمتمثلة في السلطة الفعلية في المؤسسة العسكرية، التي تتعلق بسلامة الدولة وأفرادها من العدوان الخارجي، كما ساهم في وجود أشكال جديدة من العدوان على مواطني الدولة ومؤسساتها، عبر شبكات الاتصال والمعلومات، والتي تعتمد عليها المنشآت الحيوية وهو ما يصيب الدولة بعجز في توفير الأمن على المستوى الداخلي، بحفظ سلامة الأفراد وممتلكاتهم وأموالهم، وكذلك مهمة الدفاع لعدم القدرة على تحديد مصدر الهجمات ومن ثم أخذ رد فعل سريع، كما ساعد الفضاء السيبراني في دعم الحركات الانفصالية في مواجهة الدولة، وفي التأثير على الهوية الوطنية.

- أثر الفضاء السيبراني على حق الدولة السيادي غير القابل للتصرف في تقرير نظامها السياسي والاقتصادي والثقافي والاجتماعي بحرية، وفي تنمية علاقاتها الدولية وفي ممارسة سيادتها الدائمة على مواردها الطبيعية وفقا لإرادة شعبها، دون تدخل أو تداخل، أو تخريب أو تهديد من الخارج بأي شكل من الأشكال. (عراجي، ص83-84)

- تراجع قوة الدولة القومية وتضاؤل دورها: كل الأمور السابقة أدت إلى إضعاف دور الدولة القومية، إضافة إلى ذلك أصبح من الصعب اعتبارها الفاعل الأساسي في العلاقات الدولية.

2- جدلية الاعتراف أو الإقرار بسيادة الدولة في الفضاء السيبراني

في عام 2015 أكدت الجمعية العامة للأمم المتحدة، أنه يجب على الدول احترام القانون الدولي وما يترتب عليه من حقوق وواجبات السيادة في استخدامها لتكنولوجيا المعلومات والاتصالات، بما في ذلك الفضاء السيبراني، وهذا يعني أن الدول يجب أن تطبق وتحترم كل ما ينجر عن سيادتها في كل أنشطتها في الفضاء السيبراني، وقد استندت الجمعية العامة في ذلك على أن الفضاء السيبراني لا يتواجد بدون بنية تحتية مادية مثل: "الخوادم والموزعات والكابلات"، فهي موجودة فعليا في الدول وبالتالي فهي تخضع تحت سيطرتها

ورقابتها، وبالتالي يتم تعريف السيادة السيبرانية بناءا على ذلك بأنها تطبيق مبادئ سيادة الدولة على الفضاء السيبراني.(https://bit.ly/2YcDEkQ) .

غير أن دول العالم اختلفت في ذلك فلم تعترف كلها بعد بالسيادة في الفضاء السيبراني فلكل منها سياسات وممارسات تختلف عن غيرها، حيث يعتبر البعض أن الفضاء السيبراني هو من المشاعات العالمية كالولايات المتحدة، وبالتالي لا يصح نقل السيادة إلى الفضاء السيبراني، في الوقت الذي لدى دول أخرى تصور مختلف لهذا الميدان، حيث ترى أنه يتطلب السيطرة للحد من تأثيراته وانعكاساته على أمن الدولة والمجتمع(عراجي، ص81)، كالصين، فرنسا، ألمانيا...الخ، وبالتالي تؤكد على سيادتها في الفضاء السيبراني مما خلق صراع من نوع جديد بين هذه الدول.

في هذا الإطار تعمل فرنسا بشكل جدي لتفادي أن تصبح مستعمرة رقمية للولايات المتحدة أو الصين، إذ أعلنت كل من الجمعية الوطنية ووزارة الدفاع أن أجهزتهما الرقمية ستتوقف عن استخدام محرك البحث غوغل وستستبدله بمحرك كوانت، وهو محرك بحث فرنسي وألماني يفخر بعدم تتبع مستخدميه، فقد قام وزير الدولة للشؤون الرقمية في فرنسا بالرد على قانون التكنولوجيا السحابية في الولايات المتحدة، وهو قانون جديد يسمح للولايات المتحدة بالوصول إلى البيانات المخزنة على الخدمات السحابية للشركات الأمريكية أينما وجدت في العالم، وقال أن فرنسا تستعد بالفعل للرد مع دول أوروبية أخرى على تداعيات هذا القانون.(https://bit.ly/2SklUyR) .

كما أصدرت الصين " قانون الأمن السيبراني" المعمول به منذ جوان 2017، شددت من خلاله على أنه من حق الدول ذات السيادة وضع قوانين وقواعد لتنظيم الفضاء السيبراني طبقا لما تقتضيه مصلحة البلاد. كذلك يحظى هذا النهج بشعبية أيضا لدى البلدان النامية، التي ترى نفسها في وضع رقمي غير موات ومعرضة أكثر لسلبيات للعولمة. .(https://bit.ly/2LWJLTV)

كل هذه الأمور جعلت السيادة الوطنية على المحك باعتبار امتلاك القوة الالكترونية أصبح شرطا أساسيا لتحقيق السيادة السيبرانية، نظرا لأن

الهجمات السيبرانية أصبحت سلاح قوي يهدد الدول، مما ساعد تدعيم الهيمنة الالكترونية وتغيير الخريطة الإدراكية للدولة المستهدفة وتغيير رؤيتها لمصالحها الذاتية، وهو ما كان له تأثير على كيفية تأثير الفضاء السيبراني على استخدام القوة الالكترونية عبر أدواتها المختلفة في الصراع الدولي، واستخدام القوة الناعمة عبر الدعاية وشن الحرب النفسية لممارسة الجذب وإقناع الآخرين، وتقديم الإغراءات المالية والتدريب والثقافة بما يعزز من قدرات الدول في مجال توظيف الفضاء السيبراني في خدمة الأهداف الخارجية.

وهو الأمر الذي تمارسه أمريكا من خلال احتكارها للموارد الحرجة للفضاء السيبراني، وهو ما أضاف لقوتها قوة أكبر على الهيمنة وممارستها عبر تأثيرها المباشر والعميق في شعوب العالم عبر دعم حرية الانترنت وحقوق الإنسان (عبد الصادق، ص51)، خاصةً أنّ القوة السيبرانية تتميز بقلة تكلفتها، واعتمادها على مهارات العقل البشري، مقارنة بتكاليف باهظة للقوة التقليدية الأخرى.

وبالتالي تواجه الدول تحديات عديدة أمام اعتماد سيادتها السيبرانية أهمها:

- الاعتراف بالفضاء السيبراني كمجال سيادي، وكون الدول تمارس سلطة عليه، فوجوده يتطلب هندسة مادية وبحاجة إلى قوننة، لكي يعمل بفاعلية.

- خلق نظام قادر على تحديد اللاعبين في الفضاء السيبراني بدقة، هو مهمة شاقة، نظرا لعدم القدرة على إسناد مسؤولية الهجمات الالكترونية إلى طرف محدد بنسبة 100٪، لذلك يبدو أن الدول مترددة في قبول المسؤولية عن الأنشطة الالكترونية الناشئة من أراضيها. (https://bit.ly/2YcDEkQ).

- رسم حدود الفضاء السيبراني بشكل تستطيع الدولة مراقبته والتحكم فيه، فعدم التمكن من القيام بهذه الوظيفة يفرغ الفضاء السيبراني من مضمونه.

- خلق توافق آراء بشأن ما يشكل رد فعل معقول دفاعا عن السيادة والأمن الوطني، فضعف الإسناد يزيد من عدم التأكد من مدى صحة توجيه رد

الفعل، كما يمكن يكون الرد غير معقول أو غير متكافئ.(عراجي، ص91-93).

ثانيا: مكانة السيادة السيبرانية ضمن الإستراتيجية الصينية

1- المفهوم الصيني للسيادة السيبرانية:

يتماشى ظهور موقف صيني واضح بشأن السيادة السيبرانية مع الاتجاهات الأوسع للسياسة الخارجية الصينية، فبعد سنوات من إتباع سياسة خارجية مرنة، كان ظهور الصين كقوة أكثر حزما على مدى العقد الماضي واضحا في عدة مجالات أهمها مجال الفضاء السيبراني، الذي كان ذات يوم مجالا يمكن للشركات الأمريكية أن تعمل فيه بحرية، تم استبداله بالشركات الصينية. فالموقف الصيني تغير في الدبلوماسية الدولية من نهج سلبي قائم على ردود الأفعال في الماضي إلى النهج الاستباقي إلى حد كبير ويسعى إلى استخدام نفوذه لتشكيل جدول الأعمال العالمي.(https://bit.ly/2Gj7avd).

بالنسبة للصين تعد السيادة السيبرانية جزء من مصطلح أوسع لأمن المعلومات، وهو بدوره أمر بالغ الأهمية بالنسبة للصين للحفاظ على قيمها الأساسية. في هذا الإطار أكد الرئيس الصيني "شي جين بينغ" أنه: "يجب على الدول احترام حق كل طرف في اختيار طريقته الخاصة في تطوير الانترنت، ونموذج التنظيم الالكتروني والسياسات العامة للانترنت، والمشاركة في الحوكمة الدولية على الانترنت على قدم المساواة، لا ينبغي لأي بلد أن يسعى إلى الهيمنة السيبرانية أو يتدخل في الشؤون الداخلية للدول الأخرى، أو يشارك أو يتغاضى عن أو يدعم الأنشطة السيبرانية التي تقوض الأمن القومي للبلدان الأخرى"، كما أضاف قائلا: على "أننا نأمل مع المجتمع الدولي احترام السيادة في الفضاء السيبراني، وتطوير روح الشراكة، وحل المشاكل المشتركة من خلال المشاورات، والتشجيع المشترك على التنمية، الحماية المشتركة للأمن والتمتع بالفوائد."(https://bit.ly/2Gj7avd) .

إن مفهوم الصين للسيادة السيبرانية يتعلق بهذه الطريقة بحاجتها للسيطرة على معلومات وهوية البلد والأمة، وبالتالي إدارة ومراقبة ووضع ضوابط شبكة

الانترنت الخاصة بها دون تدخل دول أخرى، وهو ليس مفهوم منفصل تماما عن الأمن السيبراني.

وفقا للصين فإن السيادة السيبرانية تعني حق كل دولة في أن تختار طريقها الخاص في الفضاء السيبراني ومن ضمن ذلك القواعد الضابطة له، وترى الصين أن ما ينبغي أن يشهده العالم هو فضاءات سيبرانية وطنية ووفق ضوابط تضعها حكومات البلدان المستقلة تحت مبدأ حقوق السيادة الوطنية لكل دولة. تعارض الصين على هذا الأساس تفرد الشركات الغربية الخاصة بالسيطرة في هذا المجال والتي تتجاوز سلطات الدول الوطنية، وقد بذلت الصين جهودا مكثفة لتأسيس فضائها السيبراني الوطني وتعتبر تعميم النموذج ضمن أولويات سياستها الخارجية..(https://bit.ly/2XQmCF6)

2- دوافع الاهتمام الصيني بالفضاء السيبراني:

تتمثل المحفزات الصينية في مجال الفضاء الإلكتروني، في الآتي:

اقتصادياً: تشمل الدوافع الاقتصادية للإستراتيجية الصينية لأمن الشبكات هدفين رئيسيين، هما: ضمان استمرار النمو الاقتصادي، وردع الجرائم السيبرانية المحلية والدولية، وذلك للتقليل من الخسائر التي تكبدها الاقتصاد الصيني، فبحسب التقديرات الحكومية بلغت الخسائر الناجمة عن الجرائم السيبرانية التي لحقت بالاقتصاد الصيني عام 2011 وحده أكثر من 830 مليون دولار، وأثرت على أكثر من 20٪ من مستخدمي مواقع الإنترنت. .(https://bit.ly/30GfEo3)

وفى النصف الأول من عام 2014 فقط، تم اختراق حوالي 6.2 مليون كمبيوتر في الصين والسيطرة عليها من عنوان بروتوكول أجنبي للانترنت (آى بى)، من بينها 2.6 مليون من هذه الكمبيوترات يتم السيطرة عليها من العناوين في الولايات المتحدة و2.4 مليون من البرتغال، وفقا لأكبر مركز لتنسيق الانترنت في الصين. (https://bit.ly/2XZPjVf).

سياسياً: السيادة الصينية في الفضاء الإلكتروني وتعزيز موقع الصين دوليا

فيما يتعلق بالدوافع السياسية تخشى الحكومة الصينية من إتاحة استخدام الإنترنت دون قيود، ومن عدم السيطرة على عملية تدفق وانتشار المعلومات

خاصةً من قِبَل المعارضة، الأمر الذي قد يشكل خطراً كبيراً على استقرار النظام الشيوعي الصيني وعلى السلطة الحاكمة، لذلك قامت الصين بتطبيق تدابير وقائية في إطار تبني مفهوم "احترام السيادة الصينية في مجال الفضاء الإلكتروني"، والذي من شأنه أن يسمح لبكين بالسيطرة على الإنترنت داخل حدود الدولة، في حين أن المفهوم الغربي للفضاء الإلكتروني يتبنى نهجاً مُنفتحاً من خلال التدفق الحر للمعلومات عبر الحدود.

كما تعتبر الصين أن وجود الكثير من البنية التحتية للإنترنت في أمريكا يعني أن إدارة الفضاء السيبراني تحت السيطرة الأمريكية. وبالتالي، فإن الهدف لا يكمن في إضافة مفهوم سيطرة الحكومة على الإنترنت اليوم واعتماد السيادة السيبرانية، ولكن إجبار أمريكا على تقاسم السيطرة التي لديها بالفعل مع دول أخرى، تتفق هذه الحجة مع الاتجاهات الأوسع في السياسة الخارجية الصينية التي تدعو إلى "دمقرطة العلاقات الدولية"، وبالتالي الابتعاد عن الهيمنة الغربية المتصورة للشؤون الدولية نحو نظام أكثر تعددية يكون للصين دورا بارزا فيه، مع احترام أكبر للحكم الذاتي والشؤون الداخلية للدول.(https://bit.ly/2YcDEkQ) .

عسكرياً: التطبيقات الإلكترونية في مجال الدفاع الوطني:

ركزت بكين على تكنولوجيا المعلومات والاتصالات من أجل توظيفها في الحروب المستقبلية، وتطمح في احتلال موقع متقدم في هذا المجال بحلول عام 2050، فقد بحث العسكريون في استراتيجيات تُمكنهم من استغلال المجال الإلكتروني في مختلف السيناريوهات الهجومية والدفاعية.

فمن المتوقع أن تلعب العمليات العسكرية الإلكترونية دوراً هاماً في السيناريوهات العسكرية المتعلقة بتايوان، والنزاعات الإقليمية والبحرية الأخرى، وكذلك ضد الولايات المتحدة. وقد أشارت العديد من التقارير الخاصة بالتهديدات المتقدمة المستمرة الصادرة عن شركات الأمن الإلكتروني الأمريكية إلى تطور مستوى الهجمات الإلكترونية الصينية ضد الحكومة والمؤسسات الصناعية والتجارية الأمريكية، على الرغم من استمرار نفي الصين لهذه الاتهامات. (https://bit.ly/2XXHURl) .

كما قامت الصين بإنشاء وحدة خاصة بالحرب الالكترونية بتطوير أسلحة نبض كهرومغناطيسية، لاستخدامها ضد حاملات الطائرات الأمريكية في أي صراع مستقبلي، وتعد هذه الأسلحة جزءا مما يعرف بمشروع أسلحة "الورقة الرابحة" لدى الصين، والتي تعتمد على التكنولوجيات الحديثة التي يجري تطويرها في مستوى عالي من السرية.(البياتي، 2014، ص274-275) .

3- إستراتيجية الأمن السيبراني الصينية:

تبنت الصين في السنوات القليلة الماضية سياسة صارمة وأكثر اتساقا تجاه الفضاء السيبراني، وفي هذا الصدد يعتبر عام 2014 عاما فاصلا حيث تم استحداث "مجموعة أمن الانترنت المركزي" و"مجموعة المعلومات الرائدة"، كلاهما تحت رئاسة الرئيس الصيني "شي جين بينغ"، وهو ما يرسل إشارة قوية على التزام الصين القوي بهذه القضية.

تنظر الصين إلى الفضاء السيبراني في الوقت نفسه على أنه تهديد كبير للاستقرار الصيني وضروري لأهداف التنمية الصينية، وبالتالي فإن تحقيق التوازن الصحيح بين الانفتاح والقمع هو مسألة حساسة. إحدى الطرق الرئيسية التي حاولت الصين تحقيق التوازن بين هاذين الشاغلين فيها كانت من خلال تشجيع الشركات المحلية ومنحها حصة في النظام، لقد تم إعطاء رجال الأعمال البارزين، مثل مؤسس "علي بابا" "جاك ما Jack Ma"، دور في تشكيل وتعزيز السياسات الصينية.(https://bit.ly/2YcDEkQ) .

كما أصدرت الصين "قانون الأمن السيبرانى الصيني" المعمول به منذ جوان 2017، شددت من خلاله على أنه من حق الدول ذات السيادة وضع قوانين وقواعد لتنظيم الفضاء السيبراني طبقا لما تقتضيه مصلحة البلاد وإتباعا للممارسات الدولية المعمول بها في هذا الصدد.

يمكن فهم قانون الأمن السيبراني في الصين، كتأثير لمفهوم السيادة السيبرانية، فجزء هام من هذا القانون يشترط أن تقوم الشركات التي تساهم في البنية التحتية الحيوية للمعلومات بتخزين بياناتها داخل الحدود الصينية. وبمقتضاه يكون محظورا على مقدمي خدمات الانترنت جمع وبيع المعلومات الشخصية للمستخدمين، كما أنه ينبغي عليهم التعامل مع هذه المعلومات بما

يتماشى مع القانون والقواعد الخاصة بالدولة، ويعطي القانون الحق لمستخدمي الانترنت أن يطلبوا من مقدمي الخدمات حذف معلوماتهم إذا ما تم إساءة استخدامها. كما يطلب القانون بامتثال الشركات لمساعدة التحقيقات الصينية، وأخيرا يستلزم المفهوم أيضا استمرار الرقابة الحالية على المواقع التي تعتبر ضارة بالصين، ومن التطورات الأخيرة قرار الحكومة اتخاذ إجراءات صارمة ضد مزودي الشبكات الافتراضية الخاصة، حيث تمكنت هذه الشبكات حتى الآن من تجنب الرقابة، مما يسمح لمستخدمي الانترنت بالوصول إلى المواقع الأجنبية المحجوبة.(https://bit.ly/2Gj7avd) .

كما تمت الاستجابة الصينية من خلال تبني إستراتيجية شاملة عام 2016 لتحقيق اكتفاء تكنولوجي ذاتي بحلول عام 2025 من خلال تخصيص مئات المليارات سنويا لأغراض تطوير القدرات الوطنية الصينية، خاصة وأنها تعتمد بشكل كامل على استيراد الرقائق الالكترونية التي تؤدي عمليات المعالجة الدقيقة، والتي تدخل في معظم الصناعات الالكترونية لأجهزة الاستخدام اليومي الشخصية والتجارية مثل الهواتف النقالة والكمبيوتر وأجهزة التلفزيون...الخ، وهي صناعات تحتل في مجملها ثلث الصادرات الصينية إلى العالم، وأخطر ما في هذا الموضوع هو الاعتماد شبه الكامل على المجهزين الأمريكيين، وقد واجهت الصين انكشافا استراتيجيا كبيرا في افريل 2018 حين قامت إدارة "ترامب" بفرض عقوبات ضريبية على شركة ZTE عملاق الصناعات الالكترونية ومعدات الاتصالات "الرابع عالميا"، مما أدى إلى توقفها بسبب إحجام المجهزين عن إمدادها باحتياجاتها، وقد تم رفع العقوبات بعد اتصالات سياسية بين البلدين، إثر ذلك قام الرئيس الصيني بتوجيه نداء خاص إلى علماء بلاده للعمل لبذل جهود استثنائية للخروج من هذا الموقف. .(https://bit.ly/2XQmCF6)

كما تبذل الصين جهودا كبيرة وتنفق الكثير لتطوير قدراتها الذاتية في ميدان حوسبة الكم، التي تستخدم ميكانيكا الكم وتوفر القدرة على إجراء عدة عمليات حساب في آن واحد، وهو حقل يحتاج إلى نوع خاص من أجهزة الحاسوب. إن إحراز التقدم في هذا المجال يؤمن للصين القدرة على تأمين

قنوات اتصال مشفرة، كما يوفر القدرة على فك شفرات الآخرين، في المجال الاقتصادي يمكن لهذه الحواسيب أن توفر منافع هائلة وخاصة في مجال تحليل المعلومات والمعطيات في معظم المجالات الصناعية. ففي عام 2016 أطلقت الصين أول قمر صناعي يمكنه نقل اتصالات مشفرة من خلال هذه الوسيلة، كما أنجزت الصين مد أطول كابل لهذا النوع من الاتصالات المشفرة بين بكين وشنغهاي. كما أعلنت الصين عام 2017 أنها تخطط لتبوأ موقع الريادة العالمية في ميدان الذكاء الاصطناعي بحدود عام 2030، وذلك بتشجيع الاستثمار والابتكار في هذا الميدان، حيث بادرت بإنشاء بعض الهيئات والشركات المتخصصة في هذا المجال، مثل: Baido شركة صينية عابرة للحدود متخصصة بخدمات الانترنت والذكاء الاصطناعي، وTencent شركة عابرة للحدود متخصصة بالانترنت والعاب الفيديو، وعملاق الانترنت Alibaba وشركة Flytex المتخصصة بجوانب دقيقة ذات صلة بالانترنت(https://bit.ly/2XQmCF6) .

كما تبذل الصين أيضا جهودا مضنية من أجل التعامل مع الموجة الجديدة من الاكتشافات وخاصة في مجال تقنيات شبكات الجيل الخامس من الهواتف النقالة، تلك التقنية الثورية الجديدة التي تعتبرها الصين العمود الفقري لإستراتيجية "صنع في الصين 2025"، التي ستحّول بكين إلى "قوة تقنية كبرى"، فيما تعتبر الولايات المتحدة تلك الإستراتيجية مصدر قلق بالغاً وتهديداً مباشراً لأمنها القومي، خاصة من طرف الشركة الرائدة عالميا "هواوي" التي تعد ثاني أكبر شركات إنتاج أجهزة الهواتف المحمولة في العالم بعد "سامسونغ" الكورية، بحصة سوقية تصل إلى 17٪ بحسب بيانات الربع الأول 2019، حيث ازدادت مبيعات هواوي عام 2018 بنسبة 20 بالمئة مقارنة مع 2017 لتصل إلى 107 مليارات دولار، بعد أن كانت 12 مليار دولار في 2008، وبذلك انتقلت إلى مصاف شركتي جوجل ومايكروسوفت الأمريكيتين للتكنولوجيا(https://bbc.in/2Ns75cH).

كما بدأت تطوير تقنية شبكة الجيل الخامس الخاصة بها في أوائل 2009، كما تصدرت تقنيات الشركة اللاسلكية لشبكة "5G" المرتبة

الأولى في اختبارات تقييم الأداء التي تتم من قبل جهات مستقلة، وفازت مؤخرا بجائزة "أفضل تقنية لشبكة الجيل الخامس" في قمة الجيل الخامس العالمية سنة 2019 (https://bit.ly/2YNNcAc). الأمر الذي أدى إلى تصعيد حدة الصراع بين الصين والولايات المتحدة التي أعلنت مقاطعتها لشركة "هوواي" ومنعتها من التنافس للفوز بعقود أمريكية، كما ضغطت على حلفائها لاستثنائها من المشاركة في شبكات الجيل الخامس فيها، وقد استجاب بعض الحلفاء لطلبها على غرار نيوزيلندا وأستراليا، فيما لا يزال حلفاء آخرون يدرسون هذه الخطوات، وأبرزهم ألمانيا وفرنسا وبولندا وبريطانيا. والسبب في ذلك حسب أمريكا يكمن في العلاقات الوطيدة التي تربط مؤسس "هواوي" بالجيش الصيني، مما يمكنه من اعتراض الاتصالات في أمريكا، كما يمكنه شن هجمات الكترونية على البنية التحتية...الخ (https://bbc.in/2Ns75cH).

وقد بلغ الصراع ذروته بين الطرفين حين اعتقلت السلطات الكندية ابنة مؤسس "هواوي" المديرة المالية "منغ وانزو"، وذلك بطلب أمريكي بتهمة الاحتيال وانتهاك العقوبات الأمريكية المفروضة على إيران، مما وتر العلاقات بين الأطراف الثلاثة خاصة بعد قبول تسليم كندا "وانزو" لأمريكا في حال ثبوت إدانتها، حيث استخدمت الصين كل إمكاناتها الدبلوماسية، وضغطت على حلفائها ومنافسيها على حد سواء، واتخذت الصين إجراءات غير اعتيادية، وانتهجت "دبلوماسية الرهائن" حيث اعتقلت مواطنين كنديين بتهمة التجسس، في محاولة لإنجاز نوع من تبادل السجناء مع كندا، ومنع تسليم "وانزو" للحكومة الأمريكية.

تشير قضية "هواوي" إلى تصاعد حدة التوترات بين الولايات المتحدة والصين، ومن غير الواضح بعد إن كان البلدان سيتجنبان المزيد من التصعيد أم أنه قد يحدث ما هو أسوأ بكثير (https://bit.ly/2Q18Pv4)، خاصة أن هناك العديد من التهم الموجهة إليها بالتحايل وسرقة أسرار تكنولوجية من الشركات الأمريكية والغربية، تحاول من خلالها الصين استدراك ما فاتها لتقليص الفجوة بينها وبين الدول الغربية المتقدمة، ليس فقط للحاق بها ولكن

لتجاوزها وادخار الكثير من الأموال والجهود في مجال البحث العلمي وقد ارتبط اسم "هواوي" بفضيحة قريبة من هذا الملف الشائك، حين اتهم أحد مهندسيها بسرقة المعلومات من روبوت لاختبار الهاتف طورته شركة T-Mobileالأمريكية. (https://bloom.bg/2rodQUj)

كما تسعى الصين لتعزيز أهدافها من خلال الدعوة إلى مفهوم السيادة السيبرانية في المحافل الدولية، "باحتواء جدول الأعمال العالمي"، أحسن مثال على ذلك هو اجتماع فريق هندسة الانترنت لعام 2015، حيث أرسلت الصين 40 ممثلا ومعظم الدول الغربية واحدا أو اثنين على الأكثر، ويتضمن الجزء الأخير من هذه الإستراتيجية بناء تحالفات وشراكات لمواجهة الهيمنة المتصورة للولايات المتحدة في هذا المجال.

حيث دافعت الصين عن فكرتها في مختلف المجالات الدبلوماسية في محاولة لإنشاء تحالف واسع من الدول يوافق على هذا المبدأ، فقد أكدت قمة "البريكيس Brics" لعام 2016 على أولوية الدول في وضع جدول الأعمال، كما دافعت الصين عن نفس الفكرة في إطار أعمال منظمة شنغهاي للتعاون، التي تتألف من الصين وروسيا والعديد من دول آسيا الوسطى، الموقف الرئيسي الذي اتخذته هذه الدول هو أولوية الدولة وإمكانية تطبيقها في مجال الفضاء السيبراني أيضا.(https://bit.ly/2Gj7avd)

إضافة إلى ذلك وفي إطار إنجاز أهدافها بتقييد نشاطات الشركات الغربية وهيمنتها على الفضاء السيبراني، فقد بادرت الصين إلى خطوات عملية من جانبها لتحقيق ذلك، حيث شرعت في إنشاء بنية تحتية هائلة لربط الصين بالمحيط الهندي والخليج العربي وأوروبا بما سماه الخبراء الصينيون "طريق الحرير الرقمي" إلى جانب مشروعها العملاق المعروف بطريق الحرير الاقتصادي، إلى جانب الطرق والجسور وخطوط السكك الحديد والمطارات فقد تم مد خطوط الألياف البصرية وشبكات الهواتف النقالة ومحطات الاتصال بالأقمار الصناعية ومراكز تجميع المعطيات والمدن الذكية... مشروع عملاق من شأنه تعزيز مكانة الصين الإستراتيجية.(https://bit.ly/2XQmCF6).

خاتمة

إن تطور وسائل الاتصالات ووسائطها ساهم في زعزعة الوظيفة التوجيهية للدولة في كل ما يتعلق بالتحكم في الفضاء السيبراني، بحيث أضحى مفهوم الحدود السياسية والجغرافية وكذلك مفهوم السيادة ومفهوم الاستقلال عن الآخرين من المفاهيم التي لا يمكن الاعتداد بها.

إذ أثرت المتغيرات الدولية التي رافقت تطور الفضاء السيبراني على مفهوم السيادة الوطنية ونطاق تطبيقه في المجالين الداخلي والخارجي على حد سواء، وقد أثارت تلك المتغيرات تحديات طالت كل أنماط الدول وطرحت نفسها بأشكال مختلفة على تلك الأنماط، وبشكل عام يمكن القول أن هناك علاقة طردية بين تأثر سيادة الدول بمتغيرات الفضاء السيبراني والتغير في مضمون الوظائف التي تقوم بها الدولة، كما يمكن القول أيضا أن هناك علاقة عكسية بين تقدم الدولة تكنولوجيا ومدى تأثرها بمتغيرات هذا الفضاء، فهناك دول مسيطرة وأخرى خاضعة، ورغم أن كل الدول بغض النظر عن موقعها سوف تعاني بشكل أو بآخر، إلا أن الدول الخاضعة تبقى الأكثر تأثرا لأن الدول القوية والمسيطرة تكنولوجيا تمتلك القدرة على توجيه مسارات التحول وتحدد قواعده، وهنا يكمن واقع العلاقة بين حماية السيادة الوطنية وضرورة تحقيق الأمن السيبراني، لذلك أضحى هذا الأخير من أولى أولويات الدول تبتكر باسمه النظريات وترسم استراتيجيات، وترصد له ميزانيات ضخمة، حيث أن مخاطر انتهاكه تتجاوز الحدود وتهدد سيادة الدول.

فمن حق كل دولة، انطلاقًا من سيادتها، وضع قوانين وقواعد لتنظيم الفضاء السيبراني طبقًا لما تقتضيه مصلحتها، وإتباعا للممارسات الدولية المعمول بها في هذا الخصوص. الأمر الذي دفع السلطات الحكومية الصينية إلى السعي الحثيث لبناء منظومة تقنية فعّالة لـ "أمن الشبكات"، في بيئة تزدهر فيها الجريمة الإلكترونية وتراخي القانون وتطبيق غير متكافئ لآلياته، لذا مثل تشريع الصين لـ"قانون الأمن السيبراني" خطوة مهمة لمعالجة هذه القضية الحساسة وتأثيرها الكبير على الأمن الوطني للدولة، ويعكس هذا القانون

اتجاهاً عالمياً واسع النطاق لتنظيم أنشطة الفضاء السيبراني ومكافحة التهديدات السيبرانية التي يمكن أن تقوض الأمن الوطني لدول العالم المختلفة.

فالصين ترى أن نطاق الفضاء السيبراني يجعل من المستحيل على ممثل واحد أن يديرها في إشارة واضحة إلى الهيمنة الأمريكية، والنتيجة هي وجود العديد من المصالح والجهات الفاعلة والإيديولوجيات التي تتصادم بشكل متكرر، قد تكون النتيجة هي منافسة متبادلة المنفعة أو يمكن أن يتحول الاحتكاك إلى صراع مدمر خاصة بين الولايات المتحدة والصين.

لذلك تسعى الصين إلى توسيع نطاق سيادتها السيبرانية وتخصص من اجل ذلك موارد هائلة خاصة في ميدان الصناعات الالكترونية، وذلك لإنشاء فضاء تتحكم فيه وطنيا الأمر الذي يخرجها شيئا فشيئا من دائرة الهيمنة والاحتكار الذي تمارسه الشركات الأمريكية في هذا المجال، وهو مجال حيوي ويمثل أفقا مستقبليا يرسم الكثير من ملامح العلاقات الدولية في العقود القادمة، ويحدد بشكل كبير نظام توازنات القوة الدولية، وبالتالي لا يمكن إرجاع دوافع تبني الصين لسيادتها في الفضاء السيبراني إلى بعد واحد فقط، بل هي أبعاد: سياسية، اقتصادية، أمنية، ثقافية، وأخرى مرتبطة أساسا بالتطلعات العالمية الصينية.

□

قائمة المراجع

باللغة العربية

الكتب:

- أبو هيف، علي صادق. (1995). القانون الدولي العام، الإسكندرية: منشأة المعارف.

- أبو جودة، الياس. (2008). الأمن البشري وسيادة الدول، بيروت: المؤسسة الجامعية للدراسات والنشر والتوزيع.

- البزاز، حسن.(2002).عولمة السيادة حال الأمة العربية، بيروت: المؤسسة الجامعية للنشر والتوزيع.

- البياتي، ياس خضير. (2014). الإعلام الجديد: الدولة الافتراضية الجديدة، عمان: دار البداية.

- خليفة، إيهاب. (2017). القوة الالكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الانترنت، القاهرة: دار العربي.

- عبد الصادق، عادل. (2016). أسلحة الفضاء الالكتروني في ضوء القانون الدولي الإنساني، الإسكندرية: مكتبة الإسكندرية وحدة الدراسات المستقبلية.

المجلات والملتقيات:

- بارة، سمير. الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر: الدور والتحديات، سياسات الدفاع الوطني بين الالتزامات السيادية والتحديات الإقليمية، ورقلة: جامعة قاصدي مرباح كلية الحقوق والعلوم السياسية، 30 و31 جانفي 2017.

- جبر، نهلة (2015). الأمن الثقافي مفهومه ودواعيه وعوامل تحقيقه. شؤون عربية. العدد 164، ص ص 134-147.

- حمدان، محمد الطيب. وخنيش، ماجدة (2018). الحروب الالكترونية وتأثيرها على سيادة الدول. مجلة الدراسات القانونية والسياسية. العدد 07، ص ص 19-34.

المذكرات:

- عراجي، أنديرا. (2016). القوة في الفضاء السيبراني: فصل عصري من التحدي والاستجابة. رسالة لنيل شهادة دراسات عليا في العلوم السياسية والإدارية. كلية الحقوق والعلوم السياسية. لبنان.

مواقع الانترنيت:

- الأمن السيبراني، https://bit.ly/2JZHEfN 08/02/2019
- الاتحاد الدولي للاتصالات، تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني، https://bit.ly/2JBgWe8 25/012019
- الأشقر جبور، منى، أهمية الاتفاقية العربية للأمن السيبراني، https://bit.ly/2XQ5NPq 21/012019
- أحمد إسماعيل، إسراء، السيادة السيبرانية: عناصر الاستراتيجية الصينية للأمن الإلكتروني، https://bit.ly/2XXHURl05/02/2019
- البار، مصطفى عدنان، والمرحبي، علي خالد، أمن المعلومات والأمن السيبراني، https://bit.ly/2LWHhFb 25/01/2019
- السعدون، فائز، الصين تحديات السيادة التكنولوجية، https://bit.ly/2XQmCF6 12/07/2019
- الشلبي، منى، الأمن السيبراني دعامة من دعائم الأمن القومي، https://bit.ly/32AYzOe 21/01/2019
- الصين: القانون الجديد للأمن السيبرانى يهدف لحماية سيادة الدولة وأمنها، https://bit.ly/2LWJLTV 08/02/2019
- الصين أكبر ضحايا الجرائم الالكترونية وتؤيد " مجتمع المصير المشترك" في الفضاء الإلكتروني، https://bit.ly/30GfEo3 11/07/2019
- الكتبي، سالم، السيادة السيبرانية والعالم الافتراضي، https://bit.ly/2JARDJc 11/07/2019
- كوانت بدل غوغل..فرنسا تريد استعادة السيادة الرقمية، https://bit.ly/2SklUyR 24/01/2019

- كيطان، أحمد يوسف، إستراتيجية الأمن الوطني السيبراني للصين: قراءة في قانون الأمن السيبراني الصيني، https://bit.ly/2XZPjVf 11/07/2019

- هل تحولت قضية هواوي إلى صراع سياسي دولي؟، https://bit.ly/2Q18Pv4 07/11/2019

- يان، تشين، لماذا يتهيب الغرب من شركة هواوي الصينية للاتصالات؟، https://bbc.in/2Ns75cH، 11/07/2019

- «5G» سباق الفضاء الجديد بين الشرق والغرب، https://bit.ly/2YNNcAc 23/08/2019

باللغة الأجنبية:

Books :

- kempf, olivier. (2015). introduction à la cyber stratégie, paris: economica.

Internet links :

- baezner, marie, and Patrice, robin, cyber sovereignty and data sovereignty, https://bit.ly/2YcDEkQ 08/02/2019

- Niels, nagelhus schia, and lars, gjesvik, the Chinese cyber sovereignty consept, https://bit.ly/2Gj7avd 10/07/2019

- Hurtado, Patricia, and Chris, Strohm, U.S. Charges Huawei With Stealing Trade Secrets, Bank Fraud, https://bloom.bg/2rodQUj 07/11/2019.